# IDENTITY THEFT

# A Quick Reference Guide



# SAN DIEGO POLICE DEPARTMENT

# PC 530.5 Unauthorized Use of Personal Identifying Information

(a) Every person who willfully obtains personal identifying information, as defined in subdivision (b), of another person without the authorization of that person, and uses that information for any unlawful purpose, including to obtain, or attempt to obtain, credit, goods, services, or medical information in the name of the other person without the consent of that person is guilty of a public offence.

# What Is Identity Theft?

Identity theft involves acquiring key pieces of someone's identifying information, such as: name, address, date of birth, social security number and/or mother's maiden name, in order to impersonate them. This information enables the identity thief to commit numerous forms of fraud which include, but are not limited to: opening

### Sample "Courtesy Notice"

(Date)

Dear (Creditor Name/Collection Agency Name)

On (Date), I received your letter demanding payment of (\$\$ amount). I did not open this account and incur this unpaid balance. Someone, other than myself, wrongfully used my personal information to obtain a line of credit/service. Your company extended a line of credit/services to someone, other than myself.

You are hereby notified that on (Date), I filed an identity theft report with the San Diego Police Dept. The case number is (xx-yyyyyy), a copy of which can be obtained by contacting the SDPD Records Section at (619) 531-2846.

Closing,

(Your name and address)

new bank accounts, taking over the victim's financial accounts, purchasing automobiles, applying for loans, credit cards and social security benefits, renting apartments, and establishing services with utility and phone companies.

## What to do if you become a victim:

- ✓ Set up a folder to keep a detailed history of this crime.
- ✓ Keep a log of all your contacts and make copies of all documents.
- ✓ Contact all creditors by phone and in writing to inform them of the problem.
   (See Sample "Courtesy Notice")
- ✓ Notify the US Postal Inspector if your mail has been stolen or tampered with:
  - US Postal Inspection Service
  - See phone listing under *Federal Government*
  - www.gov/websites.depart/inspect
- ✓ Contact the Federal Trade Commission to report the problem: <a href="www.ftc.gov">www.ftc.gov</a>
  The FTC is the federal clearinghouse for victims of identity theft. The FTC helps victims by providing information to help resolve financial and other problems that could result from identity theft. Their hotline is:
- 1-877-IDTHEFT (1-877-438-4338) ✓ Call each of the three credit bureaus'
- fraud units to report identity theft.
  Ask to have a "Fraud Alert/Victim
  Impact" statement placed on your
  credit file asking that creditors call
  you before opening any new accounts.
- Request that a copy of your credit report be sent to you.

#### **Credit Bureaus**

### **Equifax**

PO Box 74021, Atlanta, GA 30374-0241

- To order report call 1-800-685-1111
- To report fraud call 1-800-525-6285

### **Experian**

PO Box 949, Allen, TX 75013-0949

- To order report call 1-888-397-3742
- To report fraud call 1-888-397-3742

#### **Trans Union**

PO Box 390, Springfield, PA 19064-0390

- To order report call 1-800-916-8800
- To report fraud call 1-800-680-7289

- ✓ Alert your banks to flag your accounts and contact you to confirm any unusual activity.
- ✓ If you have any checks stolen or bank accounts set up fraudulently, report it to the following companies:
  - National Check Fraud Service

1-843-571-2143

- SCAN 1-800-262-7771
- TeleCheck 1-800-710-9898
- CheckRite 1-800-766-2748
- Cross Check 1-707-586-0551
- Equifax Check Systems

1-800-437-5120

- International Check Services 1-800-526-5380
- ✓ Contact the Social Security Admin. Fraud Hotline at 1-800-269-0271
- ✓ Contact the state office of the Dept. of Motor Vehicles to see if another license was issued in your name. If so, request a new license number and fill out the DMV's complaint form to begin the fraud investigation process.
- ✓ Obtain description of suspect (if known).
- ✓ Obtain witness information:
  - Persons who accepted applications
  - Salespeople
  - Apartment Managers
  - Employers

Make note of the case number in your detailed history folder and reference it when you have contact with any business or law enforcement agency concerning this report. Depending upon the jurisdiction of where the crime occurred (location where goods or services were obtained or delivered), an investigator may or may not be assigned to this case.

If the crime occurred in our jurisdiction and

there are workable leads, such as witnesses and suspect information, an investigator may be assigned to the case. Unfortunately, not all cases will be assigned to an investigator because there are not always significant leads to identify the suspect. Call the San Diego Police Department area station which provides general police services to your neighborhood to find if an investigator has been assigned to your case. Make note of the investigator's name and phone number in the space below.

### SDPD Investigator:

Phone Number:

Your SDPD Case Number is:

#### Area Stations:

C1	(10 744 0500
Central	619-744-9500
Eastern	858-495-7900
Mid-City	619-516-3000
Northeastern	858-538-8000
Northern	858-552-1700
Southeastern	619-527-3500
Southern	619-424-0400
Western	619-692-4800

#### **Preventive Actions**

- ✓ Promptly remove mail from your mailbox after delivery.
- Deposit outgoing mail in post office collection mailboxes or at your local post office. Do not leave in unsecured mail receptacles.
- ✓ Never give personal information over the telephone, such as your social security number, date of birth, mother's maiden name, credit card number, or bank PIN code, unless you initiated the phone call. Protect this information and release it only when absolutely necessary.
- ✓ Shred pre-approved credit applications, credit card receipts, bills and other financial information you don't want before discarding them in the trash or recycling them.
- ✓ Empty your wallet of extra credit cards and ID's, or better yet, cancel the ones you do not use and maintain a list of the ones you do.
- ✓ Order your credit card report from the three credit bureaus once a year to check for fraudulent activity or other discrepancies.
- ✓ Never leave receipts at bank machines, bank counters, trash receptacles, or unattended gasoline pumps. Keep track of all your paperwork. When you no longer need it, destroy it.
- ✓ Memorize your social security number and all your passwords. Do not record them on any cards or on anything in your wallet or purse.
- ✓ Sign all new credit cards upon receipt
- ✓ Save all credit card receipts and match them against your monthly bills.

- ✓ Be aware of when you normally receive your routine financial statements.
   Contact the sender if they are not received in the mail.
- ✓ Notify your credit card companies and financial institutions in advance of any change of address or phone number.
- ✓ Never loan your credit cards to anyone.
- ✓ Never put your credit card or other financial account number on a postcard or on the outside of an envelope.
- ✓ If you apply for a new credit card and it hasn't arrived in a timely manner, call the bank or credit card company.
- ✓ Report all lost or stolen credit cards immediately.
- ✓ Closely monitor expiration dates on your credit cards. Contact the credit card issuer if replacement cards are not received prior to the expiration dates.
- ✓ Beware of mail or telephone solicitations disguised as promotions offering instant prizes or awards designed solely to obtain your personal information or credit card numbers.

#### **Internet and On-Line Services**

- ✓ Use caution when disclosing checking account numbers, credit card numbers or other personal financial data at any Web site or on-line service location unless you received a secured authentication key from your provider.
- ✓ When you subscribe to an on-line service you may be asked to give credit card info. When you enter any interactive service site, beware of con artists who may ask you to "confirm" your enrollment service by disclosing passwords or the credit card number used to subscribe.
  Don't give them out!